DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Final 10/12/2021

2do cuatrimestre 2021 — Álgebra I

Integrante	LU	Correo electrónico
Yago Pajariño	546/21	ypajarino@dc.uba.ar

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

Índice

1. Final 10/12/2021

1.1. Ejercicio 1

Sea $V = \{1, 2, ..., 499, 500\}$. Se define la relación R en $P = P(V)\backslash\emptyset$ como:

$$ARB \iff min(A) = min(B) \wedge max(A) = max(B)$$

1.1.A. Demostración clase de equivalencia

Me piden probar que R es una relación de equivalencia. Por definición, una relación es de equivalencia si es reflexiva, simétrica y transitiva. Pruebo cada propuedad por separado.

Reflexividad

Por definición, R es reflexiva $\iff \forall A \in P : ARA$

Por definición de la relación,

$$ARA \iff min(A) = min(A) \wedge max(A) = max(A)$$

Dado que $A = A$ en particular, tienen el mismo mínimo y el mismo máximo. Luego R es reflexiva.

Simetría

Por definición, R es simétrica $\iff \forall(A, B) \in P^2 : ARB \implies BRA$

Por definición de la relación,

$$\begin{aligned} ARB &\iff min(A) = min(B) \wedge max(A) = max(B) \\ &\iff min(B) = min(A) \wedge max(B) = max(A) \\ &\iff BRA \end{aligned}$$

Por lo tanto $ARB \implies BRA$ como se quería probar, luego R es simétrica.

Transitividad

Por definición, R es transitiva $\iff \forall(A, B, C) \in C^3 : (ARB \wedge BRC) \implies ARC$

Por definición de la relación,

$$\begin{aligned} ARB &\iff min(A) = min(B) \wedge max(A) = max(B) \\ BRC &\iff min(B) = min(C) \wedge max(B) = max(C) \end{aligned}$$

Pero,

$$\begin{aligned} min(A) = min(B) \wedge min(B) = min(C) &\implies min(A) = min(B) = min(C) \\ &\implies min(A) = min(C) \end{aligned}$$

Y,

$$\begin{aligned} max(A) = max(B) \wedge max(B) = max(C) &\implies max(A) = max(B) = max(C) \\ &\implies max(A) = max(C) \end{aligned}$$

Por lo tanto,

$$min(A) = min(C) \wedge max(A) = max(C) \iff ARC$$

Luego R es una relación transitiva.

Por lo tanto, R es una relación de equivalencia, dado que es una relación relfexiva, simétrica y transitiva.

1.1.B. Cardinal de la clase $x = \{1, 100\}$

Busco todos los $B \in P : XRB$

Por definición,

$$\begin{aligned} XRB &\iff min(X) = min(B) \wedge max(X) = max(B) \\ &\iff 1 = min(B) \wedge 100 = max(B) \end{aligned}$$

Por lo tanto, busco todos los $B \in P(V) \backslash \emptyset : min(B) = 1 \wedge max(B) = 100$

Sabiendo que $V = \{1, 2, ..., 499, 500\}$ tengo que contar todos los subconjuntos de V que poseen al 1, poseen al 100 y no poseen ningún $a \in V : a > 100$

Por lo tanto,

- 1 tiene 1 posibilidad $\implies$ 1
- $2 - 99$ tienen 2 posibilidades $\implies 2^{98}$
- 100 tiene 1 posibilidad $\implies$ 1
- $101 - 500$ tienen 1 posibilida $\implies$ 1

Por lo tanto, habrá $1.2^{98}.1.1 = 2^{98}$ conjuntos.

Rta.: $\#\overline{\{1, 100\}} = 2^{98}$

1.1.C. Cadinal de la clase $Y = \{50\}$

Busco todos los $C \in P : YRC$

Por definición,

$$\begin{aligned} YRC &\iff min(Y) = min(C) \wedge max(Y) = max(C) \\ &\iff 50 = min(C) \wedge 50 = max(C) \end{aligned}$$

Por lo tanto, busco todos los $C \in P(V) \backslash \emptyset : min(C) = 50 \wedge max(C) = 50$

Pero el único conjunto que cumple ambas en simultáneo es $C = \{50\}$ y por lo tanto,

Rta.: $\#\overline{\{50\}} = 1$

1.1.D. Cantidad de clases de equivalencia de R

Para saber si un subconjunti de V pertenece a una clase de equivalencia, alcanza con observar el mínimo y el máximo del subconjunto.

Separo en dos casos,

(1) Clases del tipo $\{n\}$ con $n \in V$ forman 500 clases distintas y no se relacionan con subconjuntos de dos o más elementos.

(2) Clases del tipo $\{a_1, ..., a_r\} \wedge 2 \leq r \leq 500 \wedge a_i \in V$

En este caso voy a tener $500 - a_1$ clases. Por ejemplo

- $a_1 = 1 \implies \overline{\{1, 500\}}, \overline{\{1, 499\}}, \overline{\{1, 498\}}... \implies$ 499 clases.
- $a_1 = 2 \implies \overline{\{2, 500\}}, \overline{\{2, 499\}}, \overline{\{3, 498\}}... \implies$ 498 clases.
- $a_1 = 499 \implies \overline{\{499, 500\}} \implies$ 1 clase.

Luego habrá $500 + \sum_{i=1}^{499} i = 500 + \frac{499.500}{2} = 125250$ clases de equivalencia en la relación R.

1.2. Ejercicio 2

Se que $252 = 2^2.3^2.7$ y que $14 = 2.7$

Luego $(a^{255} + 10a + 1 : 252) = 14 \implies \begin{cases} 2|a^{255} + 10a + 1 \\ 4 \not| a^{255} + 10a + 1 \\ 7|a^{255} + 10a + 1 \\ 3 \not| a^{255} + 10a + 1 \end{cases}$

Ahora busco los a que cumplen cada una de estas restricciones.

Caso 2

$$\begin{aligned} 2|a^{255} + 10a + 1 &\iff a^{255} + 10a + 1 \equiv 0(2) \\ &\iff \begin{cases} a \equiv 0(2) \implies a^{255} + 10a + 1 \equiv 0 + 0 + 1 \not\equiv 0(2) \\ a \equiv 1(2) \implies a^{255} + 10a + 1 \equiv 1 + 0 + 1 \equiv 0(2) \end{cases} \end{aligned}$$

Luego $a \equiv 1(2)$

Caso 4

$a \equiv 1(2) \implies a \equiv 1(4) \vee a \equiv 3(4)$

Luego,

- $a \equiv 1(4) \implies a^{255} + 10a + 1 \equiv 1 + 2 + 1 \equiv 0(4)$
- $a \equiv 3(4) \implies a^{255} + 10a + 1 \equiv 3^{255} + 2 + 1 \equiv 9^{112}.3 + 3 \equiv 2(4)$

Luego $a \equiv 3(4)$

Caso 7

$7|a^{255} + 10a + 1 \iff a^{255} + 10a + 1 \equiv 0(7)$

Separo en dos casos: $7|a$ y $7 \not| a$ para poder usar el PTF

- $7|a \implies a^{255} + 10a + 1 \equiv 0 + 0 + 1 \not\equiv 0(7)$
- $7 \not| a \implies a^{255} + 10a + 1 \equiv (a^6)^{37}.a^3 + 10a + 1 \equiv a^3 + 3a + 1(7)$

Por lo tanto busco los $a : a^3 + 3a + 1 \equiv 0(7)$

- $a \equiv 0(7) \implies a^3 + 3a + 1 \equiv 1(7)$
- $a \equiv 1(7) \implies a^3 + 3a + 1 \equiv 5(7)$
- $a \equiv 2(7) \implies a^3 + 3a + 1 \equiv 1(7)$
- $a \equiv 3(7) \implies a^3 + 3a + 1 \equiv 2(7)$
- $a \equiv 4(7) \implies a^3 + 3a + 1 \equiv 0(7)$
- $a \equiv 5(7) \implies a^3 + 3a + 1 \equiv 1(7)$
- $a \equiv 6(7) \implies a^3 + 3a + 1 \equiv 4(7)$

Por lo tanto, $a^3 + 3a + 1 \equiv 0(7) \iff a \equiv 4(7)$

Luego $a \equiv 4(7)$

Caso 3

$$3 \not| a^{255} + 10a + 1 \iff a^{255} + 10a + 1 \not\equiv 0(3)$$

- $a \equiv 0(3) \implies a^{255} + 10a + 1 \equiv 0 + 0 + 1 \not\equiv 0(3)$

- $a \equiv 1(3) \implies a^{255} + 10a + 1 \equiv 1 + 1 + 1 \equiv 0(3)$
- $a \equiv 2(3) \implies a^{255} + 10a + 1 \equiv (a^3)^{85} + 10.a + 1 \equiv (-1)^{85} + 2 + 1 \equiv -1 + 2 + 1 \not\equiv 0(3)$

Luego $a \equiv 0(3) \vee a \equiv 2(3)$

Pero estoy buscando el resto mod 252, por lo que necesito saber $a \equiv n(9)$

Sabiendo las equivalencias mod 3, busco mod 9:

$$a \equiv 0(3) \implies a \equiv 0(9) \vee a \equiv 3(9) \vee a \equiv 6(9)$$
$$a \equiv 2(3) \implies a \equiv 2(9) \vee a \equiv 5(9) \vee a \equiv 8(9)$$

Por lo tanto, juntando todo lo hallado,

$$(a^{255} + 10a + 1 : 252) = 14 \iff \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 0(9) \vee a \equiv 3(9) \vee a \equiv 6(9) \vee a \equiv 2(9) \vee a \equiv 5(9) \vee a \equiv 8(9) \end{cases}$$

Ahora uso el Teorema Chino del Resto para hallar la equivalencia mod 252.

Busco soluciones a los sistemas $S_0 = \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 0(9) \end{cases}$ $S_1 = \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 3(9) \end{cases}$ $S_2 = \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 6(9) \end{cases}$ $S_3 = \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 2(9) \end{cases}$ $S_4 = \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 5(9) \end{cases}$
$S_5 = \begin{cases} a \equiv 3(4) \\ a \equiv 4(7) \\ a \equiv 8(9) \end{cases}$

Por TCR se que existe una única solución a cada sistema $X = x_1 + x_2 + x_3$ mod 255

Donde,

x_1 es solución del sistema $\begin{cases} a \equiv 3(4) \\ a \equiv 0(63) \implies a = 63k \implies 63k \equiv 3(4) \iff k \equiv 1(4) \end{cases}$

Luego $x_1 = 63$

x_2 es solución del sistema $\begin{cases} a \equiv 4(7) \\ a \equiv 0(36) \implies a = 36k \implies 36k \equiv 4(7) \implies k \equiv 4(7) \end{cases}$

Luego $x_2 = 36.4 = 144$

x_3 es solución del sistema $\begin{cases} a \equiv n(9) \\ a \equiv 0(28) \end{cases}$ con n el valor de mod 9 de cada S_i

- $a \equiv 0(9) \implies x_3 = 0$
- $a \equiv 2(9) \implies a = 28k \implies 28k \equiv 2(9) \implies k \equiv 2(9) \implies x_2 = 28.2 = 56$
- $a \equiv 3(9) \implies a = 28k \implies 28k \equiv 3(9) \implies k \equiv 3(9) \implies x_2 = 28.3 = 84$
- $a \equiv 5(9) \implies a = 28k \implies 28k \equiv 5(9) \implies k \equiv 5(9) \implies x_2 = 28.5 = 140$
- $a \equiv 6(9) \implies a = 28k \implies 28k \equiv 6(9) \implies k \equiv 6(9) \implies x_2 = 28.6 = 168$
- $a \equiv 8(9) \implies a = 28k \implies 28k \equiv 8(9) \implies k \equiv 8(9) \implies x_2 = 28.8 = 224$

Por lo tanto $r_{252}(a)$ serán:

- $63 + 144 + 0 = 207$
- $63 + 144 + 56 = 11$

- $63 + 144 + 84 = 39$
- $63 + 144 + 140 = 95$
- $63 + 144 + 168 = 123$
- $63 + 144 + 224 = 180$

1.3. Ejercicio 3

1.3.A. Pregunta i

Defino $f = x^2 + x + 1$ y $g = x^{2n} + x^n + 1$

Se que

$$f = \left(x - \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\right)\left(x - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\right)$$

Y se que $w_1 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$; $w_2 = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$ son raíces cúbicas de la unidad.

Por propiedades de las raíces de la unidad, se que $w \in G_n \implies w^k = w^{r_n(k)}$

Y también vale que $w \in g_3 \wedge w \neq 1 \implies 1 + w + w^2 = 0$

Por lo tanto, $f|g \iff g(w1) = 0 \wedge g(w_2) = 0$

- $n \equiv 0(3) \implies g(w_1) = w_1^0 + w_1^0 + 1 \neq 0$
- $n \equiv 1(3) \implies g(w_1) = w_1^2 + w + 1 = 0$
- $n \equiv 2(3) \implies g(w_1) = w_1^1 + w^2 + 1 = 0$

Luego $f|g \iff n \equiv 1(3) \wedge n \equiv 2(3)$

1.3.B. Pregunta ii

TODO

1.4. Ejercicio 4

$a \in \mathbb{C}$ es una raíz con $mult(a, f) = 5 \iff f = (x - a)^5.q \wedge q(a) \neq 0$

Busco el termino general de la multiplicidad de a como raíz de los polinomios de la sucesión,

- $n = 1 \implies mult(a, f_1) = 5$
- $n = 2 \implies mult(a, f_2) = 7$
- $n = 3 \implies mult(a, f_3) = 9$
- $n = 4 \implies mult(a, f_4) = 11$
- $n = 5 \implies mult(a, f_5) = 13$

Parece que la multiplicidad de a como raíz de f_n es de la forma $(n + 1)2 + 1 = 2n + 3$

Sin embargo, para poder asumir que estas multiplicidades son correctas, hay que verificar que,

$$\begin{aligned} 2n + 3 &\leq 5n \\ 3 &\leq 5n - 2n \\ 3 &\leq 3n \\ 1 &\leq n \iff n \in \mathbb{N} \end{aligned}$$

Dados h, g polinomios con $mult(\alpha, h) = 3 \wedge mult(\alpha, g) = 5 \implies \begin{cases} mult(\alpha, fg) = 8 \\ mult(\alpha, f+g) = 3 \end{cases}$

Y en el caso general, la multiplicidad de una raíz en una suma de polinomios es la de menor grado, pues $h = (x-\alpha)^3 \cdot p_1 \wedge p_1(\alpha) \neq 0$ y $g = (x-\alpha)^5 \cdot p_2 \wedge p_2(\alpha) \neq 0$ y por lo tanto, $h+g = (x-\alpha)^3 \cdot p_1 + (x-\alpha)^5 \cdot p_2 = (x-\alpha)^3(p_1 + (x-\alpha)^2 p_2)$ donde $(x-a) \not| (p_1 + (x-\alpha)^2 p_2)$

Usando esta propiedad, voy a probar por inducción que $mult(a, f_n) = 2n + 3$

Defino $p(n) : mult(a, f_n) = 2n + 3; \forall n \in \mathbb{N}$

Caso base n = 1

$$\begin{aligned} p(1) : & mult(a, f_1) = 2.1 + 3 \\ & mult(a, f_1) = 5 \end{aligned}$$

Luego $p(1)$ es verdadero.

Paso inductivo

Quiero probar que dado $h \geq 1 : p(h) \implies p(h+1)$

HI: $mult(a, f_h) = 2h + 3 \iff f_h = (x-a)^{2h+3} \cdot q_2 \wedge q_2(a) \neq 0$

Qpq: $mult(a, f_{h+1}) = 2(h+1) + 3$

Pero,

$$\begin{aligned} f_{h+1} &= (x-a)^2 f_h + f^{h+1} \\ &= (x-a)^2 f_h + ((x-a)^5 q)^{h+1} \\ &= (x-a)^2 f_h + (x-a)^{5(h+1)} \cdot q^{h+1} \\ &= (x-a)^2 \cdot (x-a)^{2h+3} \cdot q_2 + (x-a)^{5(h+1)} \cdot q^{h+1} \\ &= (x-a)^{2h+5}(q_2 + (x-a)^{5h+5-2h-5} \cdot q^{h+1}) \\ &= (x-a)^{2h+5}(q_2 + (x-a)^{3h} \cdot q^{h+1}) \end{aligned}$$

Luego $mult(a, f_{h+1}) = 2h + 5$ pues $q_2(a) \neq 0$ como se quería probar.

Por lo tanto $p(h) \implies p(h+1); \forall h \geq 1$

Luego $p(n)$ es verdadero, $\forall n \in \mathbb{N}$

Y así $mult(a, f_n) = 2n + 3; \forall n \in \mathbb{N}$